AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application.

Listing of Claims:

1. (currently amended) A system for door access control and key management, the system comprising:

(1) a door administering system for administering access to one or more doors, the door administering system having:

(a) a module for managing access privilege of one or more individuals for each door and assigning access authorization to each individual for the door,

(b) a door database for storing a door identification uniquely assigned to each door and information on each authorized individual for each door, and

(c) a module for changing data stored in the door database;

(2) a key administering system for administering one or more keys separately from the administration of the access to the door, each key being uniquely assigned to a key owner, the key administering system having:

(d) a module for managing the one or more keys and assigning a key to the key owner independently from the access privilege for each door,

[[(d)]] (e) a key database for storing one or more keys for each key owner, and

[[(e)]] (f) a module for changing data stored in the key database,

(3) a door control/lock assembly mounted on each door, the door control/lock assembly, the door administering system and the key administering system

communicating with each other through a communications network, the door control/lock assembly for identifying a user key ~~when it is~~ presented by a key user, and for operating the door based on the access privilege of the key user when the identified user key ~~of the user~~ is [[the]] a key ~~of a key owner~~ administered by the key administering system, and ~~who~~ the key user is an ~~authorized~~ individual authorized to any of the one or more doors by the door administering system and having access authorization to the door.

2-3. (cancelled)

4. (previously presented) The system as claimed in claim 1, wherein the door control/lock assembly carries out the authorization process when the communication between the door control/lock assembly and the door and key administering systems is interrupted.

5. (original) The system as claimed in claim 1, wherein the communications network includes a wireless communications network.

6. (previously presented) The system as claimed in claim 1, wherein the communications network includes an IP (Internet Protocol) communications network, and the door administering system and the key administering system include a door administering server system and a key administering server system, respectively.

7. (previously presented) The system as claimed in claim 6, wherein the door control/lock assembly and the door and key administering systems are adapted to be controlled via a web browser operatively connected to the IP communications network.

8. (previously presented) The system as claimed in claim 1, wherein the key of the key owner includes a key signature unique to the respective key owner, which is not unique to the door and is recognizable by the door control/lock assembly.

9. (previously presented) The system as claimed in claimed in claim 1, wherein the communication and authorization process between the door and key administering systems and the door control/lock assembly are carried out in a form of encrypted signals or messages.

10. (currently amended) The system as claimed in claim 1, wherein each door control/lock assembly includes;

an identification device for reading the ~~user's~~ user key presented by the key user ~~of the key~~;

a lock adapted to be operated in response to the authorization from the door and key administering systems; and

an embedded controller for controlling the operation of the identification device and the lock, and the authorization process.

11. (previously presented) The system as claimed in claim 10, wherein each key owner has one or more keys for the door, and the door control/lock assembly includes two or more identification devices which are different from each other.

12. (previously presented) The system as claimed in claim 11, wherein the key owner is authorized for access to the door by using all or several of the keys.

13. (previously presented) The system as claimed in claim 5, wherein the door control/lock assembly further includes a wireless transmitter/receiver.

14. (previously presented) The system as claimed in claim 10, wherein the door control/lock assembly further includes a module for assisting in the operation of the door control/lock assembly and sensing the status of the door, the assisting and sensing module including one or more of the following: a door open sensor, a speaker and microphone assembly, a camera, an activity light, a buzzer, a call button, a battery condition sensor, a smoke sensor, a temperature sensor.

15. (previously presented) The system as claimed in claim 10, wherein the embedded controller includes a database for storing information on the keys and users such that, when the communication between the door control/lock assembly and the door and key administering systems is interrupted, the door control/lock assembly can carry out the authorization process for the door associated therewith.

16. (previously presented) The system as claimed in claim 8, wherein the key signature includes a numeric code, a sequence of numbers, a unique signal, or a biometric recognition code.

17. (previously presented) The system as claimed in claim 1, wherein the door administering system is physically separated from the key administering system.

18. (previously presented) The system as claimed in claim 1, wherein the stored data pertaining to the doors can be updated when required by a door administrator and the stored data pertaining to the keys can be updated when required by a key administrator.

19. (previously presented) The system as claimed in claim 1, wherein the door control/lock assembly, and the door administering system and key administering system are adapted to be controlled by a web browser operatively connected to the communications network.

20. (currently amended) A method of implementing door access control and key management via a communications network, the method comprising steps of:

(1) at a door server, administering access to one or more doors, including:

(a) managing access privilege of one or more individuals for each door and assigning access authorization to each individual for the door; and

(b) at a door database, storing a door identification uniquely assigned to each door and information on each authorized individual for each door, data stored in the door database being updatable;

(2) at a key server, administering one or more keys separately from the administration of the access to the door, each key being uniquely assigned to a key owner, including:

(c) managing the one or more keys and assigning a key to the key owner independently from the access privilege for each door;

[[(c)]] (d) at a key database, storing one or more keys for each key owner, the keys being implemented by key signatures, data stored in the key database being updatable;

(3) at a door control/lock assembly, identifying a user key presented by a key user;

(4) comparing the identified user key to the keys of the key owners; and

(5) operating the door based on the access privilege of the key user by verifying that the identified user key is a key ~~of a key owner~~ administered by the key server ~~who~~ and the key user is an ~~authorized~~ individual authorized to any of the one or more doors by the door server and having access authorization to the door[[;]], ~~and~~

~~(5) operating the door based on the access privilege of the individual,~~

wherein the authorization step is carried out through the communications network between the door server and the key server.

21. (original) The method as claimed in claim 20, further comprising a step of storing two or more different unique key signatures for the user whereby all of the different key signatures are required to gain access to the door.

22. (original) The method as claimed in claim 21, wherein any one of the different key signatures is required to gain access to the door.

23. (previously presented) The method as claimed in claim 20, wherein the communications networks includes an IP communications network.

24. (previously presented) The method as claimed in claim 20, wherein the communications networks includes a wireless communications network.

25. (previously presented) A system architecture for controlling door access and key management, the system architecture comprising:

(a) a plurality of door access control and key management systems, each of which is the system for door access control and key management according to claim 1, the systems being communicatively and operatively connected to a communication network; and

(b) a Meta server being adapted to serve as an address reference among the door administering systems and the key administering systems, which are separately part of each door access control and key management system, the Meta server being communicatively and operatively connected to each of the door access control and key management systems via the communications network, wherein the Meta server contains the address of each separate door administering system and key administering system each with its associated unique key ID codes and unique door ID codes, and each door access control and key management system contains the address of the Meta server such that any key owner, whose keys are administered by any key administering system, can be granted access privileges at any door which is administered by any door administering system.

26. (original) The system architecture as claimed in claim 25, wherein the communications network includes an IP communications network.

27. (original) The system architecture as claimed in claim 25, wherein the Meta server is adapted to be controlled via a web browser communicatively and operatively connected to the Meta server through the communications network.

28. (previously presented) The system as claimed in claim 1, wherein the key owner of a key is capable of changing the key of that key owner at the key database.

29. (previously presented) The system as claimed in claim 1, wherein the door is assigned to one or more door administrators, the door administrator being capable of changing information stored at the door database and associated with the assigned doors.

30. (previously presented) The system as claimed in claim 1, wherein the door administering system is administered by one or more door administrators, and the key administering system is administered by one or more key administrators.

31. (previously presented) The system as claimed in claim 30, wherein the access given to a particular key to a particular door is communicated to the key administrator for that particular key and/or the door administrator by the door control/lock assembly.

32. (previously presented) The system as claimed in claim 1, wherein the door control/lock assembly sends the identified key to the key administering system, the door administering system or a combination thereof to obtain access authorization.

33. (previously presented) The system as claimed in claim 1, wherein the door administering system assigns, to each door, the key uniquely assigned to each key owner who is an individual having access authorization to the door.

34. (previously presented) The system as claimed in claim 33, wherein the identified key is compared with the key or keys of the key owners who are the individuals having access authorization to the door for the verification.

35. (previously presented) The system as claimed in claim 1, wherein the door administering system records authorized entries to the doors and unauthorized attempts to unlock the door.

36. (previously presented) The system as claimed in claim 29, wherein the door administering system allows the door administrator to configure a plurality of security settings for the operation of the door control/lock assembly.

37. (previously presented) The system as claimed in claim 36, wherein the security settings include a setting specifying who is authorized at specific times to the door.

38. (previously presented) The system as claimed in claim 37, wherein the security settings include a setting specifying who is to be notified in an event of an alarm and how the alarm is notified.

39. (previously presented) The system as claimed in claim 1, wherein the key database records use of the keys, including authorized access to the door and unauthorized attempt to unlock the door.

40. (previously presented) The system as claimed in claim 39, wherein the key administering system is controlled by one or more key administrators and the key administering system provides the key administrator with a report of every instance of the use of the key that has been recorded.

41. (previously presented) The system as claimed in claim 1, wherein the door administering system and/or the key administering system maintains logs of entries and exits of each user through the door.

42. (previously presented) The system as claimed in claim 41, wherein based on the logs, it is determined who is in a specific area through the door.

43. (previously presented) The system as claimed in claim 1, wherein the system gathers information which includes (i) time of attempts to access a door, (ii) an identification of a user who attempted the access, and (iii) information on attempts to gain access to the door by an unknown individual.

44. (previously presented) The system as claimed in claim 36, wherein the security setting includes access privileges of each user, which is changeable by the door administrator.

45. (previously presented) The system as claimed in claim 36, wherein the door control/lock assembly has an alarm device, which communicates with the door

administering system, the door administering system communicating with an alarm administrator in accordance with the security setting.

46. (previously presented) The method as claimed in claim 20, wherein the assigning step assigns access authorization to an individual having a key stored in the key database.

47. (previously presented) The system architecture as claimed in claim 25, wherein more than one Meta server is provided to the door access control and key management systems.